EXHIBIT I

From: Lai Yip <LYip@sheppardmullin.com>
Sent: Wednesday, April 6, 2022 12:50 PM
To: Waqas Anis <wanis@idsinc.com>; Kazim Naqvi <KNaqvi@sheppardmullin.com>; Jim Vaughn <JVaughn@idsinc.com>; Miller, Rory <Rory.Miller@lockelord.com>
Cc: Rena Andoh <RAndoh@sheppardmullin.com>; Goeke, Justine <JGoeke@gibsondunn.com>; James Fazio <JFazio@sheppardmullin.com>; Travis Anderson <TAnderson@sheppardmullin.com>; Popham, Mitchell <MPopham@lockelord.com>; Froehlich, Joseph <JFroehlich@lockelord.com>; Dominguez, Kate <KDominguez@gibsondunn.com>; Polka, Michael M. <MPolka@gibsondunn.com>; Townsend Bourne <tbourne@sheppardmullin.com>; Samplin, Ilissa <ISamplin@gibsondunn.com>; Subjeck, Melissa N. <MSubjeck@hodgsonruss.com>
Subject: RE: Moog v. Skyryse- Call re iDiscovery engagement and device protocol

And here's a PDF of the draft I just sent, which shows a few comments to the draft (not shown in the clean Word version).

Thanks,

Lai L. Yip
+1 415-774-3147 | direct
LYip@sheppardmullin.com | Bio

SheppardMullin
Four Embarcadero Center, 17th Floor
San Francisco, CA 94111-4109
+1 415-434-9100 | main
www.sheppardmullin.com | LinkedIn | Twitter

From: Lai Yip <LYip@sheppardmullin.com>
Sent: Wednesday, April 6, 2022 12:45 PM
To: Waqas Anis <wanis@idsinc.com>; Kazim Naqvi <KNaqvi@sheppardmullin.com>; Jim Vaughn <JVaughn@idsinc.com>; Miller, Rory <Rory.Miller@lockelord.com>
Cc: Rena Andoh <RAndoh@sheppardmullin.com>; Goeke, Justine <JGoeke@gibsondunn.com>; James Fazio <JFazio@sheppardmullin.com>; Travis Anderson <TAnderson@sheppardmullin.com>; Popham, Mitchell <MPopham@lockelord.com>; Froehlich, Joseph <JFroehlich@lockelord.com>; Dominguez, Kate <KDominguez@gibsondunn.com>; Polka, Michael M. <MPolka@gibsondunn.com>; Townsend Bourne <tbourne@sheppardmullin.com>; Samplin, Ilissa <ISamplin@gibsondunn.com>; Subjeck, Melissa N. <MSubjeck@hodgsonruss.com>
Subject: RE: Moog v. Skyryse- Call re iDiscovery engagement and device protocol

Counsel,

Please see attached a DRAFT protocol that addresses inspection through iDS and related issues, which would be an addendum to the Protective Order. Please let us know your comments as soon as possible.

iDS, please review also and let us know if you see any issues with the logistics proposed.

Thanks,

Lai L. Yip
+1 415-774-3147 | direct
LYip@sheppardmullin.com | Bio

SheppardMullin
Four Embarcadero Center, 17th Floor
San Francisco, CA 94111-4109
+1 415-434-9100 | main
www.sheppardmullin.com | LinkedIn | Twitter

UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF NEW YORK

MOOG INC., Plaintiff, v. SKYRYSE, INC., ROBERT ALIN PILKINGTON, MISOOK KIM, and DOES NOS. 1–50. Defendants.	Civil Action No. 1:22-cv-00187

ADDENDUM TO PROTECTIVE ORDER

This Addendum to the existing Protective Order is intended to: (1) govern Discovery Material that is made available for inspection through neutral forensic vendor iDiscovery (hereafter, "Inspection Material," as further defined below); and (2) add a new confidentiality designation, i.e., "HIGHLY CONFIDENTIAL – OUTSIDE COUNSEL & EXPERTS' EYES ONLY," which would cover Source Code and other documents as further addressed below.[1] This Addendum shall be considered part of the Protective Order as if it were fully incorporated therein.

Commented [LY1]: This would moot the need for the "HIGHLY CONFIDENTIAL – SOURCE CODE" designation in the current draft PO and we would conform the PO accordingly.

I. SCOPE OF INSPECTION MATERIAL

1. "Inspection Material" encompasses any material that is made available for inspection through iDiscovery (hereafter, "iDS"). Inspection Material may include physical devices (such as those provided to iDS in compliance with the March 11, 2022 stipulated order at Dkt. 25), all documents and materials on such devices, Source Code, and other technical

[1] All capitalized terms shall have the same meaning as those defined in the Protective Order.

documents. Inspection Material may also include documents from multiple Parties that are subject to visual comparison or analysis "side by side" so that the Parties may prosecute or defend the claims and defenses in the case.

2. The Parties recognize that a purpose of broadly defining Inspection Material is to expedite discovery and to facilitate the Parties' compliance with the Stipulation and Proposed Order re Expedited Discovery Procedures and Briefing Schedule for Preliminary Injunction Motion at Dkt. 33. However, nothing in this Addendum or the Protective Order precludes any Party from requesting that particular documentary Inspection Materials be produced (i.e., Bates stamped, designated, and served on the other Parties) as provided for in Section IV herein.[2]

II. PROVISION OF INSPECTION MATERIALS TO iDS

Inspection Materials shall be provided to iDS. iDS shall sign an "Agreement To Be Bound By Protective Order" that is attached as Exhibit A to the Protective Order.

III. REMOTE INSPECTION THROUGH iDS

All Inspection Materials capable of being remotely inspected—e.g., all electronic materials, including all those on physical devices provided to iDS—shall be made available for remote inspection through iDS.

A. Forensic Imaging of Inspection Materials to Be Inspected

1. iDS shall make forensic images of all Inspection Materials, and only such forensic images will be subject to inspection by the Receiving Party, in order to maintain the forensic integrity of the originals. The Producing Party shall provide iDS with any usernames,

[2] Nor does this Addendum preclude any Party in this action from seeking further order of this Court, including modification of this Order, or from objecting to discovery that the Party believes to be improper.

access passwords, decryption keys, two-factor authentication codes, or other information needed to allow iDS to perform the forensic imaging and other procedures as provided in this Addendum and the Protective Order.

2. **Collection of Data Pertaining to Physical Devices.** For all Inspection Materials that are physical devices, iDS shall (i) take clear photographs of devices from all angles with sufficient detail to show markings and text; and (ii) record the specifications and serial number identifiers, including internal/embedded serial numbers, for the devices to document their current state and physical properties. This information shall be made available to the Receiving Party as part of the forensic image of the physical device for remote inspection (see Section III.B.1 herein).

3. **Preparing Target Media for Forensic Image.** iDS shall properly prepare suitable forensic target media for receipt of any forensic images or forensic collections created through iDS's execution of any directives under this Addendum and the Protective Order, by wiping the forensic target media or by using new forensic target media not previously used.

4. **Forensic Imaging Process.** iDS shall make two (2) identical physical forensic bit-stream images, or forensically sound collections for accounts or devices incapable of having a full bit-stream copy made, of all Inspection Materials onto separate electronic media (the "Forensic Images"): One forensic copy shall remain untouched as a backup image; a second forensic copy shall be used as a "working copy" for inspection and review. The original Inspection Materials shall, at all times, be preserved unaltered. The imaging will be accomplished through the use of industry-standard equipment and best practices methodology

and shall include the generation of MD5 hash values or other industry standard hash values (if applicable) to demonstrate each image and file's authenticity.

B. Setup of Inspection Laptops

1. iDS will load the "working copy" forensic images of Inspection Materials (see Section III.A.4 herein) as well as any data collected as part of those forensic images (see Section III.A.2 herein) onto a read-only folder (the "Inspection Materials Folder") on a virtual machine that is hosted by iDS and remotely accessible using remote inspection laptops ("Inspection Laptops"). iDS shall provide these Inspection Laptops, set them up for use by Authorized Reviewers (as defined below), and manage these Inspection Laptops. Inspection Laptops will not contain any Inspection Materials locally; instead, all Inspection Materials will be available in the Inspection Materials Folder on iDS's virtual machine and remotely accessible using the Inspection Laptops.

2. To ensure integrity of the inspection, the same Inspection Materials Folder will be accessible to all Authorized Reviewers, through the Inspection Laptops, who are provided access under this Addendum and the Protective Order. Each Party may also work with iDS to create a folder on the virtual machine that is accessible only to the Inspection Laptops assigned to their Authorized Reviewers, but inaccessible to the Inspection Laptops assigned to other Parties' Authorized Reviewers, for notes and work product. Such notes and work product shall comply with Sections III.F.2 and III.F.3 herein. Each Party may request that iDS securely export and transmit its Authorized Reviewers' notes and work product from the virtual machine to the Party.

3. Each Inspection Laptop will have a camera that will permit and facilitate remote monitoring of inspections by iDS, as described in Section III.E herein.

C. Distribution of Inspection Laptops

1. Each Receiving Party will receive at least four Inspection Laptops and no more than eight, along with the login/password credentials necessary to access those Inspection Laptops, to distribute as it sees fit amongst its Outside Counsel and Experts who have been approved in accordance with the terms herein and in the Protective Order. *Only* such Outside Counsel and Experts shall have access to the Inspection Laptops, and shall be referred to herein as "Authorized Reviewer(s)."

2. iDS shall deliver each Inspection Laptop to an Authorized Reviewer only via hand carry, Federal Express, or other similarly reliable courier to a location mutually agreed upon by the Parties. Each Inspection Laptop may not be removed from this location, except to be returned to iDS via hand carry, Federal Express, or other similarly reliable courier, after providing notice to iDS and the Producing Party of the intended shipment and receiving confirmation from iDS that such shipment can be securely received.

D. Maintaining Security of Inspection Laptops and Inspection Materials

1. Each Inspection Laptop will be restricted such that there is no internet access beyond the domains necessary for remote access to the Inspection Materials, use of any review or inspection tools, and videoconference monitoring services. Except as provided for in Section III.D.2 herein, each Inspection Laptop will also be configured to disable all USB connections, screenshots, screen sharing, copy/paste, or other ability to transfer any data off of the Inspection Laptops.

2. An Inspection Laptop may be configured to connect to additional monitors to facilitate the inspection and review.

3. When an Inspection Laptop is not in use, it must be turned off and kept within a locked safe or a locked room (including a secure closet or cabinet) within the office or home of Authorized Reviewers when not in use. Any Authorized Reviewer who is to receive an

Inspection Laptop shall, prior to receipt thereof, provide the Producing Party with details regarding the location at which the Inspection Laptop will be used for inspection and the location at which such computer will be stored when not being used for reviewing, for the sole purposes of ensuring compliance with the requirements of this Addendum and the Protective Order.

4. Any inspection should be conducted from a private place such as a home or office to ensure that only those who have agreed to this Addendum and the Protective Order have access to the Inspection Laptops. While any Inspection Laptop is in use, no one other than an Authorized Reviewer may be permitted in the room where the inspection is occurring, and the Inspection Laptop's screen shall be positioned in such a way that it is not visible from any external window of the room in which it is stored, or such window shall be covered with blinds, shades, or a similar covering.

5. iDS shall configure all Inspection Laptops to align with NIST SP 800-171.

6. IDS shall configure all Inspection Laptops to include a "splash screen" that requires an Authorized Reviewer to confirm that she or he is a U.S. citizen and an Authorized Reviewer and to acknowledge that the Inspection Laptop provides access to highly confidential information and Source Code, which may include Controlled Unclassified Information and export controlled information that can only be accessed by U.S. citizens.

7. When an inspection is not taking place, iDS shall disable all accounts with remote access to the Inspection Materials Folder on the virtual machine.

8. When an inspection has been "idle" for fifteen (15) minutes, the Authorized Reviewer will automatically be logged out for security purposes. However, the account will not be disabled until the close of the inspection period as specified in Section III.E.1 herein.

9. During an inspection, all Inspection Materials accessed through the Inspection Laptop shall be deemed and treated as "HIGHLY CONFIDENTIAL – OUTSIDE COUNSEL AND EXPERTS' EYES ONLY." As addressed in Section IV herein, if a Receiving Party requests production of any Inspection Materials and such Inspection Materials are produced, the production will be designated appropriately and as applicable pursuant to this Addendum and the Protective Order.

Commented [LY2]: Section IV.4.1(a) of the current draft PO, which discusses treatment of materials that are inspected, would have to be conformed accordingly.

10. Once the inspection is complete, the Authorized Reviewer must log out of his or her account and the Inspection Laptop.

E. Monitoring Use of Inspection Laptops

1. When the Receiving Party wishes to inspect the Producing Party's Inspection Materials, the Receiving Party shall provide notice of one (1) business day to iDS and the Producing Party. Such notice shall include the estimated start time of the review, estimated duration of the review, identification of the Inspection Laptop(s) that will be used, and identification of the Authorized Reviewer who will be inspecting the Producing Party's Inspection Materials. Inspection will occur on a business day during the hours of 9:00AM through 9:00PM Eastern Time. iDS, at its discretion, may agree to accommodate reasonable requests to conduct inspections at other times.

2. Prior to the start of any inspection, iDS will send a videoconference invite (e.g., a Zoom invite) to the Authorized Reviewer specified in Section III.E.1 herein. At the beginning of the inspection, the Authorized Reviewer will connect to the videoconference using the Inspection Laptop and present a government-issued picture identification card to a representative of iDS (the "Inspection Supervisor"). Once the Inspection Supervisor has verified the identity of the Authorized Reviewer and that no other individuals are able to see the screen of the Inspection Laptop, the Authorized Reviewer's account will be enabled and the Authorized

Reviewer may log on to the virtual machine from the Inspection Laptop and access the Inspection Materials Folder.

3. The Receiving Party shall keep the visual stream of the videoconference connected through the duration of the inspection. The visual stream of the Authorized Reviewer will be recorded through the duration of the inspection. The videorecording shall be kept and maintained by iDS. To reduce costs, the Inspection Supervisor will not visually monitor the Authorized Reviewer through the duration of the review. Instead, after the inspection is complete, the Inspection Supervisor will "fast forward" or "scrub" through the videorecording to ensure that the Authorized Reviewer's inspection has complied with the provisions of this Addendum and the Protective Order (e.g., that unapproved reviewers are not in the room where the inspection is occurring, the screen of the Inspection Laptop is not being photographed, etc.). The purpose of this monitoring is only to ensure that there is no conduct occurring that is prohibited by this Addendum or the Protective Order. The Inspection Supervisor is not permitted to report on any activities of the Authorized Reviewers other than as may relate to the above-referenced purpose of the monitoring.

4. The Inspection Laptop's camera shall remain on the Authorized Reviewer through the duration of the inspection, but the camera need only be positioned to observe the conduct of the Authorized Reviewer in the room and shall not be positioned to see the Authorized Reviewer's precise keystrokes or what files the Authorized Reviewer is accessing on the Inspection Laptop. The microphone on the Inspection Laptop may be muted during the inspection.

5. The Inspection Laptops and the accounts shall be configured so that the Producing Party may not monitor, or determine, directly or indirectly: (i) the portions of

Inspection Material viewed by the Receiving Party; or (ii) the parameters or results of any searches or analyses performed by the Receiving Party.

F. Taking Notes and Creating Work Product During Remote Inspection

1. During remote inspection of Inspection Materials, the Receiving Party may take notes and create work product about the Inspection Materials on another electronic device (i.e., besides the Inspection Laptop) or on paper. This other electronic device may be networked.

2. The notes and work product shall comply with Section III.H herein, and shall not be used to recreate the Producing Party's Inspection Materials for use outside of the inspection. The notes and work product shall also be subject to the use and disclosure provisions of this Addendum and the Protective Order. In particular, the notes and work product shall be designated in accordance with the designations of the Protected Materials that are the subject of the notes and work product. For example, if the Protected Materials are designated "HIGHLY CONFIDENTIAL – OUTSIDE COUNSEL AND EXPERTS' EYES ONLY," then notes and work product about those Protected Materials shall likewise be designated "HIGHLY CONFIDENTIAL – OUTSIDE COUNSEL AND EXPERTS' EYES ONLY." If the Protected Materials are Inspection Materials that have not yet been produced and designated pursuant to Section IV herein, then the notes and work product shall be designated "HIGHLY CONFIDENTIAL – OUTSIDE COUNSEL AND EXPERTS' EYES ONLY" until such production and designation.

3. The notes and work product shall be subject to all applicable privileges.

G. Communications During Inspection

During the inspection and while in the room where the inspection is occurring, the Authorized Reviewer may not call, videoconference, email, text, chat, or otherwise communicate

with others except other Authorized Reviewers. The Authorized Reviewer may also communicate with the Inspection Supervisor during the inspection as provided for in Section III.E herein.

H. No Reproduction of Inspection Material from Inspection Laptop

1. Except as provided for in Section IV herein, the Receiving Party shall not email, upload, download, copy, or electronically transmit or electronically store any Inspection Materials from the Inspection Laptop (including, but not limited to, through use of a camera or imaging device). The Inspection Laptop shall not be connected to a printer in any way.

2. The Parties recognize that adherence to Section III.H.1 and other protections in this Addendum and the Protective Order are necessary to ensure the Inspection Materials receive adequate protection. For a Receiving Party to use Inspection Material outside of the Inspection Laptop, the Inspection Material must be produced and properly designated by the Producing Party in accordance with Section IV herein.

I. Tools for Use During Remote Inspection

iDS may load select software tools, agreed on by the Parties, on the virtual machines remotely accessible through the Inspection Laptops. These software tools may include, but are not limited to, word processing tools such as Microsoft Word, Excel, and PowerPoint; PDF viewers such as Adobe Reader or Acrobat; text editors such as Notepad++; comparison tools such as WinDiff and UltraCompare; source code IDEs such as Visual Studio; Cygwin tools; Understand from SciTools; SQLite Expert; utilities to unzip and uncompress files such as 7-Zip; multifile search tools such as UltraEdit; Cellebrite Physical Analyzer; and Cellebrite Inspector (formerly known as Blacklight). To be clear, the foregoing identified tools are merely examples and the Parties expect that more tools will be identified. The Parties agree that iDS may "whitelist" certain IP addresses and/or URLs if needed for functionality of the software tools. To

the extent iDS does not already have fully and appropriately licensed copies of the software tools that can be used in the inspection, the Party wishing to use such tools is responsible for providing the tools to iDS. Under no circumstances will a trial version of a software tool be used. In no event shall the Receiving Party use any compilers, interpreters or simulators in connection with the Producing Party's Inspection Materials.

IV. REQUESTING PRODUCTION OF INSPECTION MATERIALS

1. Except as provided for in Section IV.2 herein, the Receiving Party may request production of documentary Inspection Materials. The Receiving Party shall provide to the Producing Party the precise file path, file name, page numbers, and line numbers (as applicable) for any Inspection Materials that Receiving Party requests to be produced. Subject to Section IV.3 herein, the documentary Inspection Materials to be produced shall be Bates numbered and designated appropriately and as applicable pursuant to the Protective Order and this Addendum, and served within five (5) business days of the Receiving Party's request.

2. The Receiving Party shall not request production of Source Code in order to review Source Code outside of the Inspection Laptop in the first instance, as the parties acknowledge and agree that the purpose of the protections herein would be frustrated by such a request. Production of Source Code is permitted solely to enable use of such Source Code in filings, depositions, proceedings, contentions, expert reports, and related drafts and correspondence.

3. If the Producing Party objects to production of Inspection Materials, the parties must promptly meet and confer. If the Parties cannot resolve the objection, the Producing Party must file a request within five (5) business days to prevent production of any requested Inspection Materials. Otherwise, the requested Inspection Materials shall be produced. The Receiving Party must file a response within five (5) business days of the Producing Party's filing

of the request. The burden shall be on the Producing Party to demonstrate that such production is more than is reasonably necessary for a permitted purpose. Provided a request is timely filed, any contested Inspection Materials need not be produced to the Receiving Party until the matter is resolved by the Court. The procedures of this Paragraph may be modified by the Court.

V. USE OF INSPECTION LAPTOPS AT DEPOSITIONS OR HEARINGS

A Receiving Party may request that an Inspection Laptop be made available for use in a deposition or pretrial hearing by notifying the Producing Party and iDS of its intent to do so at least five (5) business days before the deposition or pretrial hearing. Following such notification, the Receiving Party may bring an Inspection Laptop to the deposition or pretrial hearing, and iDS will be prepared to provide access to the virtual machine through the Inspection Laptop during the deposition or pretrial hearing. The monitoring and communication requirements described in Sections III.E and III.G herein are inapplicable to any inspection taking place during a deposition or hearing where the Producing Party is present.

VI. IN-PERSON INSPECTION AT iDS

To the extent any in-person inspection of physical materials at the offices of iDS becomes necessary in this action, the parties will promptly confer on a protocol regarding same.

VII. COMMUNICATIONS WITH iDS

1. The Parties shall not engage in *ex parte* communications with iDS, with the exception of: (i) oral communications between an Authorized Reviewer and an Inspection Supervisor during the monitoring process described in Section III.E herein; (ii) to orally configure or troubleshoot licensing issues with respect to the software tools to be used for inspection; or (iii) as expressly permitted elsewhere in this Addendum and the Protective Order.

2. When a Producing Party provides Inspection Materials to iDS, the Producing Party must simultaneously notify all the other Parties regarding this provision (e.g., by